

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

A BLACK APPLE IPHONE, WHICH IS CURRENTLY IN  
THE CUSTODY OF THE PHILADELPHIA POLICE  
DEPARTMENT

Case No. 23-MJ-1042

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. §§ 2119, 924(c),  
and 922(g)

Offense Description

Carjacking, use of a firearm during and in relation to a crime of violence, and felon in possession of a firearm

The application is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Jung Yim

Applicant's signature

Jung Yim, FBI Task Force Officer

Printed name and title

Sworn to before me and signed telephonically.

Date: \_\_\_\_\_



Digitally signed by ETH Signature  
Date: 2023.05.23 15:28:14 -04'00'

Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Elizabeth Hey, U.S.M.J.

Printed name and title

## UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania 

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )

Case No. 23-MJ-1042

A BLACK APPLE IPHONE, WHICH IS CURRENTLY IN  
THE CUSTODY OF THE PHILADELPHIA POLICE  
DEPARTMENT )

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Eastern District District of Pennsylvania  
(identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):  
See Attachment B (incorporated by reference)**YOU ARE COMMANDED** to execute this warrant on or before June 6, 2023 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to \_\_\_\_\_  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: \_\_\_\_\_

Digitally signed by ETH  
SignatureDate: 2023.05.23 15:28:36  
-04'00'City and state: Philadelphia, PA

Honorable Elizabeth Hey, U.S.M.J.

Printed name and title

**Return**Case No.:  
23-MJ-1042

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**IN THE UNITED STATES DISTRICT COURT**

**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

**IN THE MATTER OF THE SEARCH OF  
A BLACK APPLE IPHONE, WHICH IS  
CURRENTLY IN THE CUSTODY OF  
THE PHILADELPHIA POLICE  
DEPARTMENT**

**Magistrate No. 23-MJ-1042**

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Jung Yim, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – one electronic device – which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation (“FBI”) assigned to the Philadelphia, Pennsylvania Division. I have been a Task Force Officer of the FBI for two years. I am currently assigned to the Philadelphia Violent Crime Task Force and have been for approximately the past two years. In the course of my work, I have participated in investigations of violations of federal law committed by violent offenders, including robberies, assaults on federal law enforcement, firearms offenses, and other violent crimes.

3. This affidavit is based upon my personal knowledge, experience and investigation, as well as information related to me directly or through reports of other FBI agents and task force officers, Philadelphia Police Department personnel and other law enforcement officers in the course of their official duties. Throughout this affidavit, reference will be made to “agents,” referring to those federal, state and local law enforcement officers who have directly

participated in the investigation, and with whom I have had regular contact. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not included all information known by me or other agents concerning this investigation. I have set forth only those facts I believe are essential to establish the probable cause for the search warrant. This affidavit does not exhaust my knowledge or that of other agents of the facts and circumstances surrounding this investigation.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that AZIER PUGH has committed violations of 18 U.S.C. §§ 2119 (carjacking); 18 U.S.C. § 924(c)(1)(A) (use of a firearm during and in relation to a crime of violence); and 18 U.S.C. § 922(g)(1) (felon in possession of a firearm).<sup>1</sup>

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

5. The property to be searched is a black Apple iPhone, currently in the possession of the Philadelphia Police Department (“PPD”) in Philadelphia, Pennsylvania and assigned property receipt number 3603039 in case 23-25-013669. This phone belonged to AZIER PUGH and was seized during his arrest on March 7, 2023 (hereinafter referred to as the “DEVICE”).

6. The applied-for warrant would authorize the forensic examination of this DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

---

<sup>1</sup> AZIER PUGH was indicted on these three charges on May 16, 2022, by a grand jury sitting in the Eastern District of Pennsylvania, based on a carjacking committing on March 7, 2023. The criminal case number related to this indictment is 23-CR-219.

**PROBABLE CAUSE**

7. On March 7, 2023, at approximately 6:10 p.m., an armed carjacking occurred inside Hunting Park in Philadelphia, Pennsylvania (“PA”), in the area of 1000 Lycoming Street. Hunting Park is an approximately 87-acre park in North Philadelphia, which contains sports fields and recreation areas. The victim (hereinafter referred to as “Victim 1”)<sup>2</sup> was an 18-year-old male who was leaving baseball practice with his coach and teammates. As Victim 1 approached his car, an unknown male, later identified by police as AZIER PUGH (“PUGH”), approached, pointed a handgun at the coach and then pointed the gun at Victim 1 and demanded Victim 1’s car keys. Victim 1 gave PUGH his keys, and PUGH got into Victim 1’s car and drove away. Victim 1 described PUGH as a black male, medium build, wearing a black ski mask and a black North Face jacket, armed with a handgun that was silver on top and black on bottom.<sup>3</sup>

8. Victim 1’s car was a red 2022 Kia Sportage, bearing PA license plate HCW8483, Vehicle Identification Number KNDPM3AC9N7984454. The National Insurance Crime Bureau has informed me that Victim 1’s car was manufactured in South Korea.

9. Victim 1 quickly reported the carjacking to PPD. Less than 15 minutes after the carjacking, PPD officers observed Victim 1’s car driving in the area of Broad Street and Pike

---

<sup>2</sup> Victim 1 has not been identified by name in order to ensure his safety given the violent nature of this investigation. Victim 1 has been interviewed by law enforcement and his narrative of the crime is believed to be truthful and credible as aspects of his information have been corroborated by independent means of this investigation. Victim 1 provided information to law enforcement as a victim/witness to crime and not in anticipation of receiving any financial compensation, or prosecutorial or judicial consideration in connection with any pending criminal matters.

<sup>3</sup> Victim 1 stated that, before driving away, PUGH walked back to Victim 1, lowered his mask and stated, “You don’t have to be scared.” Victim 1 indicated, however, he did not get a good look at PUGH’s face.

Street (approximately 0.5 miles from the carjacking location). PPD officers got behind the car and the driver (later identified as PUGH) made a sudden turn, striking another occupied car. PUGH continued driving and led PPD officers on a chase at a high rate of speed, until he was blocked by another car on a one-way street (the 4200 block of Bodine Street). PUGH got out of Victim 1's car and ran, without putting the car in park. PPD officers chased PUGH on foot and eventually stopped him on top of a low-level building roof after he climbed a wall covered in barbed wire.<sup>4</sup> PUGH initially provided the fake name of Rasheed Thomas, but was eventually identified as AZIER PUGH, date of birth June 29, 1998.<sup>5</sup>

10. At the time of his arrest, PUGH was wearing black clothing and had a black ski mask in his hand. PUGH also had the following items on his person: 33 loose, sealed pink plastic baggies containing a clear white rocky substance suspected of being crystal methamphetamine, and a plastic baggie with 27 blue flip-top jars containing a white chunky substance suspected of being crack cocaine. An analysis completed by the City of Philadelphia Police Department Office of Forensic Science confirmed the substances recovered to be Methamphetamine/Cocaine and Cocaine Base, respectively.<sup>6</sup>

---

<sup>4</sup> Before he was apprehended, PUGH stood on the ledge of the low-roof (approximately one story) and threatened to jump off the roof and screamed at the officers to call his mom, which the officers did. An officer was able to grab PUGH by his belt area and pull him off the ledge of the roof and arrest him. In a prison call PUGH made from local custody on March 16, 2023, PUGH indicated that although the officers probably thought he really meant to kill himself, he did not. PUGH said in the call he was just stalling for time because he did not want to get arrested.

<sup>5</sup> After PPD arrested PUGH, officers brought Victim 1 to the scene. Victim 1 stated he was unable to identify PUGH at that time. He later told detectives PUGH looked familiar, but he was not sure.

<sup>6</sup> In a prison call PUGH made from local custody on March 16, 2023, PUGH indicated he was "high" on the day of the carjacking.

11. While officers were securing PUGH on the low roof, other PPD officers secured Victim 1's car and, in the back seat, recovered a black North Face jacket (which did not belong to Victim 1 and was consistent with Victim 1's description of the jacket worn by PUGH). Inside the jacket pockets, officers located a black Apple iPhone (the DEVICE) and a Kahr Arms model P9 9mm handgun, serial number ED7398, loaded with one 9mm round in the chamber and nine 9mm rounds in the magazine (ten total rounds). The gun was silver on top and black on bottom, consistent with the description given by Victim 1. A Special Agent from the Bureau of Alcohol, Tobacco, Firearms and Explosives has informed me that the firearm was not manufactured in the Commonwealth of Pennsylvania.

12. I reviewed Philadelphia Department of Prisons audio phone calls made by PUGH after his arrest by Philadelphia Police on March 7, 2023. These calls all begin with an automated warning that they are being recorded and monitored. In several calls, PUGH discussed the carjacking. In a call on March 16, 2023, PUGH described how he committed the carjacking, the car chase from police, the car accident where he struck another car during the chase, the foot pursuit, and his eventual arrest on the low building roof. PUGH indicated, in summary, that he was walking through Hunting Park when he first saw a Maserati Truck he had wanted, but then saw Victim 1 playing baseball in the park, and Victim 1's red Kia parked nearby. PUGH said about Victim 1, "I jam him for the wheel<sup>7</sup>...." Pugh also said he was wearing snow pants, a ski mask, a black North Face jacket and Nike ACG shoes at the time of the robbery. PUGH also says

---

<sup>7</sup> I believe this is a colloquial phrase meaning he carjacked the victim for the car (I know that "wheel" is a common term for a car based on my training and experience).

that when he jumped out of the carjacked car, he left the North Face jacket in the car, which had the gun<sup>8</sup> in the pocket.

13. PUGH's criminal history indicates that he was convicted of a felony robbery offense and a related felony firearm offense in 2019, making him ineligible to possess a firearm.

14. I believe probable cause exists that the DEVICE contains evidence of the offenses under investigation in this case. Based on my training and experience, I know that people who engage in violent crime commonly utilize their cellular telephones to communicate with co-conspirators (including via text message) to facilitate, plan, and execute their crimes.<sup>9</sup> For example, I know that individuals involved in violent crime often store contact lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their cellular telephones, to be used in furtherance of their violent crime activities. Further, I am aware that people who engage in carjackings and robberies will often use the internet (including on their cell phones) to search for information about their intended victims and/or information about the cars they intend to steal or have stolen. Further, I am aware that people who engage in carjackings and robberies often possess photographs and videos (including in their phones) of themselves and their co-conspirators/accomplices; the victims of their crimes;

---

<sup>8</sup> PUGH refers to the gun as a "gat," which I know to be a common term for a gun based on my training and experience.

<sup>9</sup> In the present case, Victim 1 and other witnesses only described PUGH participating in the carjacking. However, based on my training and experience, I know it is common for people who commit carjackings to work with co-conspirators who are not directly present at the scene of the carjacking, and therefore would not be visible to witnesses. Co-conspirators could include people acting as a lookout for law enforcement; as a driver who brought the carjacker to the scene of the carjacking; or as a purchaser of the carjacked car (if the carjacker was intending to sell the car). Searching the DEVICE will assist law enforcement in determining whether PUGH was working with such a co-conspirator.

clothing worn during the crimes; weapons and other items used during the crimes; the proceeds of their crimes; and items purchased with the proceeds of the crimes. I am also aware that people who illegally possess firearms often communicate with others regarding those firearms, including by texting photos of the firearms or posting photos of the firearms to social media.

15. The DEVICE is currently in the lawful possession of PPD – it was placed into evidence at PPD and was assigned Property Receipt number 3603039 in case number 23-25-013669. It came into PPD’s possession in the following way: The DEVICE was seized from the black North Face jacket that was worn by PUGH and left in Victim 1’s car (the same jacket where police also located the gun). Therefore, while the FBI might already have all necessary authority to examine the DEVICE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the DEVICE will comply with the Fourth Amendment and other applicable laws.

16. Based on the above, I submit there is probable cause to believe AZIER PUGH has committed violations of 18 U.S.C. §§ 2119(1), (carjacking); 18 U.S.C. § 924(c)(1)(A) (use of a firearm during and in relation to a crime of violence); and 18 U.S.C. § 922(g)(1) (felon in possession of a firearm), and that evidence of these violations exists in the DEVICE.

#### **TECHNICAL TERMS**

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with

other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the

antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit

accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **Pager:** A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that the DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

19. Based on my training and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensic tools. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

20. I also know from my training and experience that criminals, including those who engage in violent carjackings, often have multiple phones to facilitate their commission of illegal activities or to attempt to thwart identification by law enforcement through the use of “burner” phones which cannot be traced back to an individual. Based on my training and experience, I know that individuals involved in violent crime also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, individuals involved in violent crime often keep old phones. I am aware that those involved with violent crimes often keep old cellular telephones at their residences, or other locations rented/owned by them, to allow the individuals to restore contacts into newer cellular telephones. I am also aware that individuals involved in violent crime often utilize pre-paid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of a third

person, in order to mask their direct linkage to telephones utilized in furtherance of the individuals' illegal activities.

21. Based on my training and experience, I know that those involved in violent crime communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in violent crime communicate with associates using cellular telephones and computers to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

22. In addition, individuals involved in violent crime sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their illegal activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

23. In addition, I know that those involved with violent crime often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, i.e. photographs of accomplices and/or individuals common to co-conspirators. I am also aware that individuals involved in violent crime often use their cellular telephones to take and/or possess photographs or videos of the victims of their crimes; items used or obtained during the crimes; the proceeds of their crimes; and items purchased with the proceeds of the

crimes. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

24. Furthermore, based on my training and experience, I am aware that individuals involved in violent crime often use a cellular phone's Internet browser for web browsing activity related to their illegal activities. Specifically, individuals involved in violent crime may use an Internet search engine to search for information about the victims of their crimes and/or media coverage of their crimes. Individuals involved in violent crime may also use the Internet to make reservations for travel related to their illegal activities. In addition, I know that individuals involved in violent crime also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, and to display weapons, items obtained from violent crimes and proceeds from criminal activity, or to post photographs of locations where they have traveled in furtherance of their illegal activities.

25. In addition, individuals involved in violent crimes sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their illegal activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located. Based on my training and experience, I am aware that individuals involved in violent crime often maintain messages, notes, ledgers and/or other records relating to their travel, their crimes and transportation.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of Examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant. Searching for the evidence described in Attachment B to the search warrant may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the device using whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

28. *Manner of Execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is good cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

s/Jung Yim

Jung Yim  
Task Force Officer  
Federal Bureau of Investigation

Subscribed and sworn to before me on May \_\_\_\_\_, 2023

Digitally signed  
by ETH Signature  
Date: 2023.05.23  
15:29:21 -04'00'



HONORABLE ELIZABETH HEY  
United States Magistrate Judge

**ATTACHMENT A**

**ITEMS TO BE SEARCHED**

The property to be searched is a black Apple iPhone, currently in the possession of the Philadelphia Police Department and assigned property receipt number 3603039 in case 23-25-013669 (hereinafter the “DEVICE”).

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying and seizing the electronically stored information described in Attachment B.

**ATTACHMENT B**

**PARTICULAR THINGS TO BE SEIZED**

1. All records that relate to violations of 18 U.S.C. §§ 2119(1) (carjacking); 924(c)(1)(A) (use of a firearm during and in relation to a crime of violence); and 18 U.S.C. § 922(g)(1) (felon in possession of a firearm); and involve AZIER PUGH and other unknown subjects, between March 5 and March 7, 2023, including:
  - a. Documents in electronic form, including correspondence, records, opened or unopened emails, text messages, voicemail messages, call logs, chat logs, internet history, note files, GPS data and map history pertaining to the planning or commission of carjackings and robberies; the possession of firearms or ammunition; and the distribution, expenditure or location of proceeds of the above-listed crimes.
  - b. Photographs, videos, audio files or other records relating to the planning or commission of the above-listed crimes and/or the possession of firearms or ammunition, including photographs of AZIER PUGH and his co-conspirators/accomplices; the victims of their crimes; clothing worn during the crimes; weapons and other items used during the crimes; the proceeds of their crimes; and items purchased with the proceeds of the crimes.
  - c. Address books and calendars.
2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including, but not limited to the following:

- a. Forms of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.
- b. Data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed, converted, stored, concealed, or transmitted, or similar computer impulses or data.
- c. Stored electronic information and communications, including but not limited to, telephone or address directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, and telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; store audio; and stored video.
- d. Evidence and contents of logs and files on the device, such as those generated by the device’s operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the device at the time any actions relating to the above offenses were taken.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.